

Position-Based Quantum Cryptography using Entanglement Swapping

Muhammad Nadeem^{1, a)}

1. School of Electrical Engineering and Computer Science, National University of Sciences and Technology H-12 Islamabad, 44000, Pakistan.

(Dated: 1 April 2014)

Various authors proposed position-based quantum cryptographic protocols, identification and position verification of a prover by sending and receiving quantum signals from various verifiers at distant reference stations. Buhrman et al showed that all PBQC protocols, where prover's position is his only credential, are insecure if eavesdroppers are allowed to share an arbitrarily large entanglement. So it is obvious to ask whether PBQC is still feasible if prover and verifier possess some classical data secret from the adversary, instead of communicating all information through public channel. Here we propose a PBQC protocol based on entanglement swapping. It is shown that our protocol is unconditionally secure even in the presence of eavesdroppers with unbounded quantum information power provided prover and one of the verifier share some secret entangled data. In case of multiple reference stations, our protocol can be used as QKD protocol.

PACS numbers: 03.67.-a

I. INTRODUCTION

Quantum cryptography offers unconditional security through quantum key distribution [1,2] in communication [3,4,5]. Our prime focus in this paper is to propose an information theoretic position-based quantum cryptographic protocol. The first quantum scheme for position verification was proposed by Kent, Munro, Spiller and Beausoleil in 2002 under the name of "quantum tagging" and later US patent granted in 2006 [6]. The central task of position-based cryptography introduced by Chandran et al [7] is position verification; a prover proves to a set of verifiers located at certain distant reference stations that he/she is indeed at a specific position. They proved that unconditional security in classical PBC is impossible because of cloning. The eavesdroppers can copy classical information, manipulate and send response to verifiers before honest prover without even noticed by prover and verifiers.

In quantum setting, number of position-based quantum cryptographic protocols has been presented [6][8-12]. But Buhrman et al [13] have proved that if honest prover doesn't not share any secret information with verifiers, nor he has any advantage over eavesdroppers beyond his position in the environment fully controlled by eavesdroppers with arbitrarily large pre-shared entanglement, then no information-theoretic PBQC is possible at all. They proved that security of any PBQC protocol can be destroyed by eavesdroppers through teleporting quantum states back and forth and performing instantaneous nonlocal quantum computation, an idea introduced by Vaidman [14]. However, in [13], it is showed that if eavesdroppers do not share any entanglement (NO-PE model), then secure position-based cryptography is possible. Moreover, since all known attacks on PBQC are based upon entanglement shared among eavesdroppers,

so motivation for recent research in this area is to find threshold of entanglement for secure PBQC. H. K. Lau and H. K. Lo [11], proposed a security proof for a scheme that relies on the assumption that the adversaries share entanglement in the form of a two- or three-level system. In [15], it is showed that if eavesdroppers possess an exponential (in n) amount of entanglement then they can successfully attack any PBQC scheme where verifiers share secret n -bit string.

Similarly, it is also interesting to know whether PBQC is still feasible if prover and verifiers possess some classical data secret from the adversary, instead of communicating all information through public channel. Kent [12] claimed that secure PBQC is possible if prover and verifiers pre-share some classical bit string unknown to eavesdroppers who have unlimited power of receiving, transmitting and manipulating quantum and classical information. Continuing the same line of research, we showed in this paper that PBQC can be made unconditionally secure by sharing entangled states between one of distant verifier and prover. We use the idea of entanglement swapping, prover P and other verifiers who were not correlated initially can be made entangled through entanglement swapping protocol [16]. Our protocol defines a new and simple application of entanglement swapping in PBQC. We will show that our protocol can be used as secure key distribution protocol in case of multiple verifiers. Our paper is organized as follows. In section II, we discuss entanglement swapping while in section III, we will introduce our PBQC protocol based on entanglement swapping. Finally, we discuss security of our protocol and summarize the paper in section IV.

II. ENTANGLEMENT SWAPPING

Entanglement swapping [16] is an interesting extension of teleportation, in fact, teleportation of entanglement. It causes two quantum particles to become nonlocally correlated even if they have never interacted. Let Alice possess

^{a)} Electronic mail: muhammad.nadeem@seecs.edu.pk

two particles 1 and 2 and Bob has particle 3 while Charlie keeps particle 4 in his possession. Moreover, suppose Bob and Charlie never met with each other (particles 3 and 4 are initially uncorrelated) but Bob's particle 3 is entangled with Alice's particle 1 while Charlie's particle 4 is entangled with Alice's particle 2 in one of Bell's state:

$$|\psi_{u_i u_j}\rangle_{\pm} = \frac{1}{\sqrt{2}}(|u_i\rangle|u_j\rangle \pm |1 \oplus u_i\rangle|1 \oplus u_j\rangle)$$

Where u_i and $u_j \in [0, 1]$ and \oplus denotes addition with mod 2. By performing Bell state measurement (on her particles 1 and 2) on the initial state of four particles 1, 2, 3 and 4;

$$\begin{aligned} |\psi_{u_1 u_3}\rangle_+ \otimes |\psi_{u_2 u_4}\rangle_+ &= \frac{1}{2}(|u_1\rangle|u_3\rangle|u_2\rangle|u_4\rangle + \\ &|u_1\rangle|u_3\rangle|1 \oplus u_2\rangle|1 \oplus u_4\rangle + |1 \oplus u_1\rangle|1 \oplus u_3\rangle|u_2\rangle|u_4\rangle + \\ &|1 \oplus u_1\rangle|1 \oplus u_3\rangle|1 \oplus u_2\rangle|1 \oplus u_4\rangle) \end{aligned}$$

Alice can project Bob and Charlie's particles (3 and 4) into one of the four possible Bell states:

$$\begin{aligned} |\psi_1\rangle &= \frac{1}{\sqrt{2}}(|u_1\rangle|u_2\rangle + |1 \oplus u_1\rangle|1 \oplus u_2\rangle) \otimes \frac{1}{\sqrt{2}}(|u_3\rangle|u_4\rangle + |1 \oplus u_3\rangle|1 \oplus u_4\rangle) \\ |\psi_2\rangle &= \frac{1}{\sqrt{2}}(|u_1\rangle|u_2\rangle - |1 \oplus u_1\rangle|1 \oplus u_2\rangle) \otimes \frac{1}{\sqrt{2}}(|u_3\rangle|u_4\rangle - |1 \oplus u_3\rangle|1 \oplus u_4\rangle) \\ |\psi_3\rangle &= \frac{1}{\sqrt{2}}(|u_1\rangle|1 \oplus u_2\rangle + |1 \oplus u_1\rangle|u_2\rangle) \otimes \frac{1}{\sqrt{2}}(|u_3\rangle|1 \oplus u_4\rangle + |1 \oplus u_3\rangle|u_4\rangle) \\ |\psi_4\rangle &= \frac{1}{\sqrt{2}}(|u_1\rangle|1 \oplus u_2\rangle - |1 \oplus u_1\rangle|u_2\rangle) \otimes \frac{1}{\sqrt{2}}(|u_3\rangle|1 \oplus u_4\rangle - |1 \oplus u_3\rangle|u_4\rangle) \end{aligned}$$

Initially, entangled pairs were (1, 3) and (2, 4). But after Bell state measurement by Alice, irrespective of outcome, entangled pairs are (1, 2) and (3, 4). You can say that particles 3 and 4, initially uncorrelated, become nonlocally correlated through entanglement swapping. In order to complete the protocol, Alice will have to communicate two classical bits (say) to Bob, who can then share a definite bell state $|\phi_{u_3 u_4}\rangle$ with Charlie after applying suitable unitary local transformation. Bose, Vedral, and Knight [17] generalized this protocol to multiparticle entanglement swapping. They showed how to create an N-particle entangled state given an M-particle entangled state.

III. OUR PBQC PROTOCOLS

We assume that honest prover's location and verifier reference stations are secure from adversary; they can store quantum data, process, and keep data secret. We also assume that the reference stations are trusted and known to each other; communications between them is secure. However, quantum/classical channels between prover and verifiers are not secure. Moreover, there is no bound on storage, computing, receiving and transmitting powers of eavesdroppers. In short, eavesdroppers have full control of environment except prover's location, reference stations, and quantum channel between verifiers. We assume that all reference stations and prover have fixed position in Minkowski space-time where all have precised and synchronized clocks. And finally, we suppose that signals can be sent between distant reference sta-

tions and between prover and reference stations at the speed of light. While the time for information processing at prover's location and reference stations is negligible. For simplicity, we will discuss protocol for one honest prover P and two reference stations R_1 and R_2 . Let two reference stations are d distance apart and prover is also at a distance d from each reference station R_1 and R_2 ; verifiers and P are at the vertices of an equilateral triangle of sides d as shown in Figure 1. Explicit procedure of our protocol follows:

1). R_1 prepares two 2-qubit entangled states

$$\begin{aligned} |\psi_{u_1 u_2}\rangle_{R_1 R_2} &= \frac{1}{\sqrt{2}}(|u_1\rangle|u_2\rangle \pm |1 \oplus u_1\rangle|1 \oplus u_2\rangle) \\ |\psi_{u_1 u_2}\rangle_{R_1 P} &= \frac{1}{\sqrt{2}}(|u_1\rangle|u_2\rangle \pm |1 \oplus u_1\rangle|1 \oplus u_2\rangle) \end{aligned}$$

Where u_1 and $u_2 \in [0, 1]$ and \oplus denotes addition with mod 2. R_1 keeps first qubit of both entangled state with her while prover P and verifier R_2 pick second qubit from $|\psi_{u_1 u_2}\rangle_{R_1 P}$ and $|\psi_{u_1 u_2}\rangle_{R_1 R_2}$ respectively.

2). R_1 performs entanglement swapping by local operations on her qubits shared in states $|\psi_{u_1 u_2}\rangle_{R_1 R_2}$ and $|\psi_{u_1 u_2}\rangle_{R_1 P}$ such that verifier R_2 gets entangled with P. R_1 communicate with R_2 , two classical bits $u_1 u_2 \in (00, 01, 10 \text{ or } 11)$, such that R_2 share a definite bell state $|\phi_{u_1 u_2}\rangle_{R_2 P}$ with P after applying suitable unitary local transformation.

3). At $t = 0$, R_1 sends a qubit rotated through angle $(-1)^{u_1 \oplus u_2} \pi/4$ to both P and R_2 simultaneously.

4). Both P and R_1 can know the values of u_1 and u_2 with certainty, say by sending qubit and Bell state measurements. Moreover, they can apply X gates on their

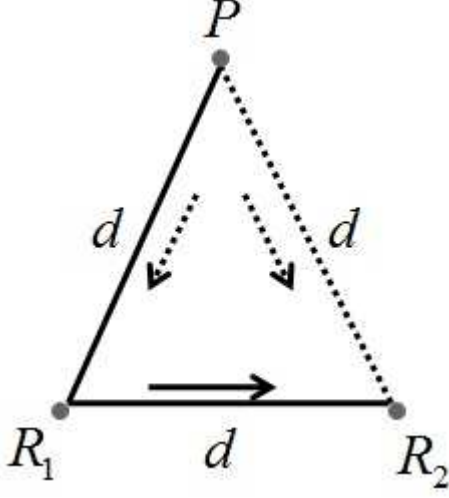


FIG. 1. Solid lines show pre-shared entanglement while dashed line represents entanglement through entanglement swapping. Solid arrow shows communication of two classical bits while dashed arrows shows responses from P to verifiers R_1 and R_2 .

entangled qubits and then Z gates simultaneously. Because both $X \otimes X$ and $Z \otimes Z$ commute with each other and act as parity operator on the Bell states:

$$\begin{aligned} |\phi_{u_1 u_2}\rangle &= \frac{1}{\sqrt{2}}(|0\rangle|u_2\rangle + (-1)^{u_1}|1\rangle|1 \oplus u_2\rangle) \\ X \otimes X |\phi_{u_1 u_2}\rangle &= (-1)^{u_1} |\phi_{u_1 u_2}\rangle \\ Z \otimes Z |\phi_{u_1 u_2}\rangle &= (-1)^{u_2} |\phi_{u_1 u_2}\rangle \end{aligned}$$

5). P decrypts the rotated qubit (inverse rotation through $(-1)^{u_1 \oplus u_2} \pi/4$ with classical two bit string $u_1 u_2$ (one of four possible 00, 01, 10 or 11 values) and sends outcome to both R_1 and R_2 simultaneously.

6). If both verifiers at stations R_1 and R_2 agree, identity of P is validated from the announced results. Besides, the position of P can be verified by checking the time elapsed for response from P, $t = 2d/c$, after sending encrypted qubit.

If $N+1$ verifiers located at distant reference stations R_2, R_3, \dots, R_{N+1} are entangled with verifier at station R_1 , who is also entangled with prover P, through 2-qubit bell state then a secure secret key of length $2N$ can be generated between P and R_1 .

IV. SECURITY ANALYSIS AND SUMMARY

Security of our protocol relies on the fact that there is nothing for the eavesdroppers to intercept process/teleport and try to prove them as honest prover. Our protocol remains unconditionally secure even if

eavesdroppers have infinite amount of pre-shared entanglement and power of non-local quantum measurements in negligible time. None of the verifiers will send any secret information which would help in decrypting encoded qubit through public channel. We also want to highlight that our protocol is different from one given by Malaney [9,10]. He used multiparticle entangled states shared between verifiers but P was not entangled with any of the verifier. Moreover, in [9,10], different verifiers communicate information about encryption scheme to P through public channel. While in our protocol, nothing is sent publically to P but encrypted data only. Our protocol is in the line of research proposed by Kent [12], who proposed to share some secret information between P and one of verifier not known to eavesdroppers. That secret data can be then used as a secret key. Moreover, in Kent protocol [12], other stations still need to communicate some secret information publically. We too, suppose that some entanglement is shared between P and R_1 but not a single bit of information helpful in decryption of encrypted data is communicated publically with P. Our protocol can be extended to more than two reference stations by using multiparticle entanglement swapping [17]. Moreover, our protocol can be used as QKD scheme in case of large number of reference stations.

- [1] C. H. Bennett and G. Brassard, Quantum cryptography: in Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, pages 175-179, 1984.
- [2] A. K. Ekert, Phys. Rev. Lett., 67, 661 (1991).
- [3] D. Mayers, Journal of the ACM (JACM) 48, 406 (2001).
- [4] H. K. Lo and H. F. Chau, Science 283, 2050 (1999).
- [5] P. W. Shor and J. Preskill, Phys. Rev. Lett., 85, 441 (2000).
- [6] A. P. Kent et al, 2006, US patent US20067075438.
- [7] N. Chandran et al. In CRYPTO 2009, pages 391-407. Springer, 2009.
- [8] A. Kent, B. Munro, and T. Spiller. Phys. Rev. A, 84, 012326 (2011).
- [9] R. A. Malaney. Phys. Rev. A, 81(4):042319, Apr 2010.
- [10] R. A. Malaney. in Global Telecommunication Conference (GLOBECOM 2010), 2010 IEEE. 10.1109/GLOBECOM.2010.5684009.
- [11] H. K. Lau and H. K. Lo. Phys. Rev. A, 83(1):012322, Jan 2011.
- [12] A. Kent. Phys. Rev. A 84, 022335 (2011).
- [13] H. Buhman et al. in Advances in Cryptology - CRYPTO 2011 - 31st Annual Cryptology Conference, Vol. 6841 (2011) p. 423.
- [14] L. Vaidman. Phys. Rev. Lett., 90(1): 010402, Jan 2003.
- [15] S. Beigi and R. Konig. New Journal of Physics 13 (2011) 093036.
- [16] M. Zukowski et al, Phys. Rev. Lett. 71, 4287 (1993).
- [17] S. Bose, V. Vedral, and P. L. Knight, Phys. Rev. A 57, 822 (1998).